### **Policy 9: Privacy and Data Sharing Policies**

#### **Introduction**

This policy outlines how the issuer collects, uses, shares, and protects cardholders’ personal and transaction data. It describes cardholder rights, data-sharing practices, and the steps taken to ensure the security and privacy of cardholder information.

#### **Section 1: Data Collection**

* **Types of Data Collected**: The issuer collects several types of information, including:
  + **Personal Information**: Name, address, Social Security number, date of birth, and income.
  + **Transaction Information**: Purchases made with the card, including amounts, locations, and merchants.
  + **Account Information**: Payment history, credit usage, account balances, and credit limit.
  + **Device Information**: IP address, browser type, and device settings when using the mobile app or online portal.
* **Sources of Data**: Data is collected directly from the cardholder during account application, through transaction records, and via third-party partners such as merchants, data brokers, and credit reporting agencies.

#### **Section 2: Use of Collected Data**

* **Primary Uses**: Collected data is used to:
  + Process transactions and manage cardholder accounts.
  + Monitor for fraud and unauthorized activity.
  + Improve customer service and personalize the cardholder’s experience.
  + Provide targeted offers and promotions.
* **Secondary Uses**: With cardholder consent, data may be used for:
  + Marketing purposes, including personalized ads and offers.
  + Analytical purposes, such as improving fraud detection models or optimizing credit risk assessments.

#### **Section 3: Data Sharing with Third Parties**

* **Affiliates**: The issuer may share personal and account information with its affiliated companies for marketing and operational purposes. Cardholders can opt out of sharing for marketing purposes by contacting customer service.
* **Non-Affiliates**: Data may also be shared with non-affiliated third parties, such as:
  + **Service Providers**: Companies that process payments, provide fraud monitoring, or deliver account services.
  + **Merchants**: Sharing of transaction data for loyalty programs, rewards, and promotional offers.
  + **Legal Requirements**: The issuer may disclose data to comply with federal and state laws, court orders, or government requests.
* **Opt-Out for Marketing**: Cardholders can opt out of having their data shared with third parties for marketing purposes by submitting a request via the issuer’s privacy center. Opting out does not affect necessary operational data sharing.

#### **Section 4: Data Security and Protection**

* **Encryption and Security Measures**: The issuer uses industry-standard encryption to protect cardholder data during transactions and when stored in its systems. Additional security measures include:
  + **Multi-Factor Authentication**: For accessing sensitive information or conducting high-risk transactions.
  + **Real-Time Fraud Monitoring**: Continuous monitoring of transactions for suspicious activity.
  + **Data Masking**: Personal data, such as Social Security numbers and card numbers, are masked in communications and databases unless explicitly needed for a transaction.
* **Data Retention Policy**: The issuer retains cardholder data for as long as necessary to fulfill the purposes outlined in this policy or as required by law. Once data is no longer needed, it is securely destroyed.

#### **Section 5: Cardholder Rights**

* **Right to Access**: Cardholders have the right to request a copy of the personal data the issuer holds about them. Requests can be submitted via the issuer’s online portal or by contacting customer service.
* **Right to Correct**: Cardholders can request corrections to any inaccurate personal data. The issuer will investigate and, if necessary, update the data within **30 days** of receiving the request.
* **Right to Delete**: In certain circumstances, cardholders may request the deletion of their personal data. This right may be limited if the issuer is required by law to retain certain data (e.g., transaction records for fraud prevention).
* **Right to Opt Out of Data Sharing**: Cardholders can opt out of data sharing for non-operational purposes by submitting a request via the issuer’s privacy center.

#### **Section 6: Cookies and Tracking Technologies**

* **Use of Cookies**: The issuer uses cookies and other tracking technologies on its website and mobile app to:
  + Track browsing activity for analytical purposes.
  + Personalize content and ads for cardholders.
  + Monitor website performance and prevent fraud.
* **Cookie Management**: Cardholders can manage their cookie preferences via their browser settings or through the issuer’s privacy center. Disabling cookies may limit certain functionalities of the website or app.

#### **Section 7: Data Breach and Incident Response**

* **Data Breach Notification**: In the event of a data breach that exposes cardholder information, the issuer will notify affected cardholders within **72 hours** of discovering the breach. Notifications will include details about the breach, the data exposed, and steps cardholders can take to protect their information.
* **Remediation Efforts**: Following a breach, the issuer will implement remediation measures, which may include offering free credit monitoring services, issuing new cards, and enhancing security protocols.

#### **Section 8: Changes to Privacy and Data Sharing Policies**

* **Policy Amendments**: The issuer reserves the right to amend this privacy and data sharing policy with **30 days' notice**. Changes will apply to future data collection and sharing practices.
* **Notification of Changes**: Cardholders will be notified of any changes via email, the online portal, or postal mail. Changes that materially affect cardholder rights (e.g., new data-sharing practices) will be highlighted.

#### **Section 9: Legal Compliance**

* **Compliance with Laws**: The issuer complies with all relevant privacy laws, including:
  + **Gramm-Leach-Bliley Act (GLBA)**: Regulates the sharing of financial information.
  + **California Consumer Privacy Act (CCPA)**: Provides additional rights to cardholders residing in California.
  + **General Data Protection Regulation (GDPR)**: Applies to cardholders in the European Union and includes specific rights such as data portability and erasure.

#### **Section 10: How to Contact Us**

* **Privacy Inquiries**: Cardholders can contact the issuer’s privacy office via email, phone, or postal mail for inquiries or to exercise their privacy rights.
  + **Email**: [privacy@issuer.com](mailto:privacy@issuer.com)
  + **Phone**: 1-800-PRIVACY
  + **Mailing Address**: Privacy Office, 123 Card Issuer St., City, State, ZIP Code